www.pwc.com

Hack.lu 2012
23-25 October
It can only be attributable to human error.

Insecurity of security equipments

Eric Chassard
Maxime Clementz

pwc

Speakers

Eric Chassard and **Maxime Clementz** belong to the Ethical Hacking team from the IT Consulting department at PwC Luxembourg.

Eric (+20 years of experience) is mainly responsible for managing projects linked to IT security. He also assumes a technical expert role in the field of IT security.

Maxime (@maxime_tz) just got his master's degree from the TELECOM Nancy (ESIAL) school. Besides working on this subject about security equipments, Maxime is now improving his skills in ethical hacking, pentesting, reverse engineering…

Discussion

How it started

We encountered such **physical security equipments** on several occasions during regular **IT pentests** (not *physical* pentests).

They captured our attention because the **technologies** used are not unfamiliar to us.

When we first **managed to exploit** such a system on a **real case study**, we decided to dig for more **security flaws** within other market solutions.

Physical security is an **universal** problem whereas we did not find any relevant papers in the **hacking community**.

Discussion

“Insecurity of security equipments”

Our topic is about equipments used for **physical security** such as surveillance cameras, fire detection, access control systems, intrusion detection…

We **will not focus** on how those equipments could be defeated but **how they could ruin** the security level of a whole organisation.

Indeed, those equipments are increasingly sold as turnkey solutions, deeply integrated within the existing IT network.

We will show that those equipments are often **overlooked** when it comes to IT Security, probably because of the thought: “**it’s secure because it’s for security**”.

Spectacular hacking of doors & cameras in Hollywood movies: fact or fiction?

1

```
struct group_info init_groups = { .usage = ATOMIC_INIT(2) };
struct group_info *groups_alloc(int gidsetsize){
    struct group_info *group_info;
    int nblocks;
    int i;

    nblocks = (gidsetsize + NGROUPS_PER_BLOCK - 1) / NGROUPS_PER_BLOCK;
    /* Make sure we always allocate at least one indirect block pointer */
    nblocks = nblocks ? : 1;
    group_info = kmalloc(sizeof(*group_info) + nblocks*sizeof(gid_t *), GFP_USER);
    if (!group_info)
        return NULL;
    group_info->ngroups = gidsetsize;
    group_info->nblocks = nblocks;
    atomic_set(&group_info->usage, 1);

    if (gidsetsize <= NGROUPS_SMALL)
        group_info->blocks[0] = group_info->small_block;
    else {
        for (i = 0; i < nblocks; i++) {
            gid_t *b;
            b = (void *)__get_free_page(GFP_USER);
            if (!b)
                goto out_undo_partial_alloc;
            group_info->blocks[i] = b;
        }
    }
    return group_info;

out_undo_partial_alloc:
    while (--i >= 0) {
        free_page((unsigned long)group_info->blocks[i]);
    }
    kfree(group_info);
    return NULL;
}

EXPORT_SYMBOL(groups_alloc);

void groups_free(struct group_info *group_info)
{
    if (group_info->blocks[0] != group_info->small_block) {
        int i;
        for (i = 0; i < group_info->nblocks; i++)
            free_page((unsigned long)group_info->blocks[i]);
    }
    kfree(group_info);
}

EXPORT_SYMBOL(groups_free);

/* export the group_info to a user-space array */
static int groups_to_user(gid_t __user *grouplist,
              const struct group_
```

ACCESS GRANTED

Hollywood phy-sec hacking scenes
Jurassic park (1993)

The girl, *Lex* (Ariana Richards), uses the Unix computer to **close a gate** on a hungry dinosaur.

Hollywood phy-sec hacking scenes

Mission: impossible (1996)

Luther Stickell (Ving Rhames) helps *Ethan Hunt* (Tom Cruise) by **triggering the fire alarm** of a whole building's floor, **from a truck, outside**.

Hollywood phy-sec hacking scenes
Ocean's eleven (2001)

The vault, common to the three casinos owned by *Terry Benedict* (Andy Garcia) in Las Vegas has its **CCTV streams hijacked** by the team assembled by *Danny Ocean* (George Clooney).

Hollywood phy-sec hacking scenes

Ocean's eleven (2001)

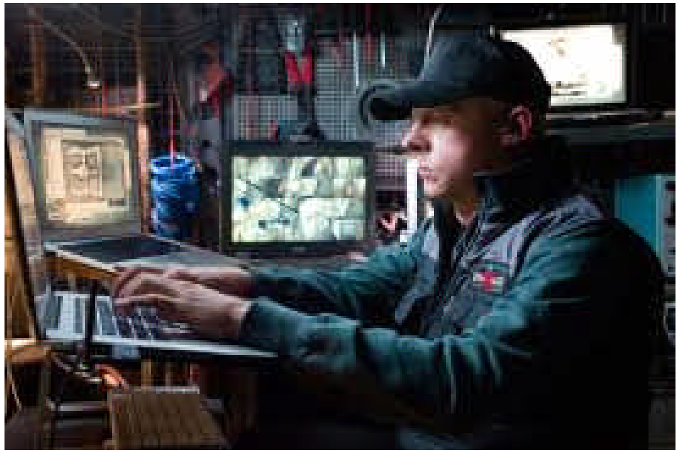
The vault, common to the three casinos owned by *Terry Benedict* (Andy Garcia) in Las Vegas has its **CCTV streams hijacked** by the team assembled by *Danny Ocean* (George Clooney).

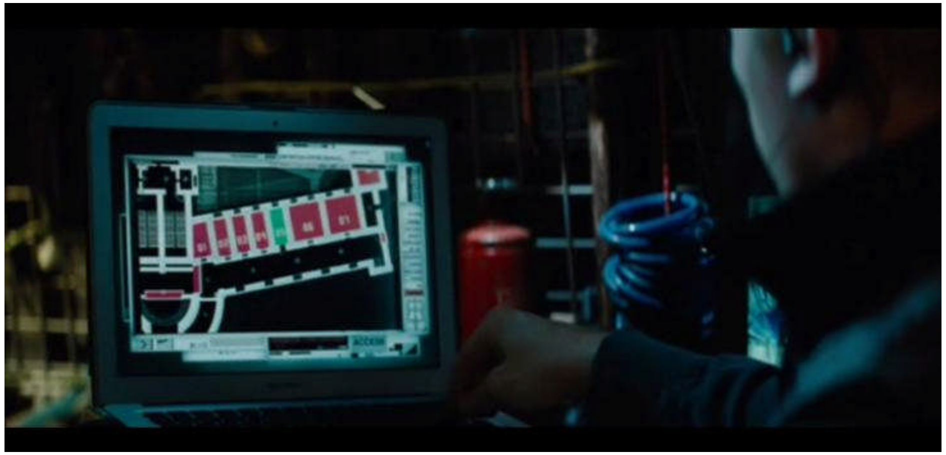
Already discussed:

- in a Sweden student project report (Cristopher Dahlstöm)
- at **Defcon 17** (2009) : "Advancing video application attacks with video interception, recording, and replay" (Jason Ostrom & Arjun Sambamoorthy)

Hollywood phy-sec hacking scenes
Mission: impossible - Ghost protocol (2011) ***1/2***

- *Benji* (Simon Pegg) hacks the system to **open the cell gates** and to **lock** the guards' **doors**. He **spies the CCTV streams** to see what's going on in the jail.
- He also **plays a song** on the jail's speakers… And does all of it **remotely**, sitting in his van **from the street**!

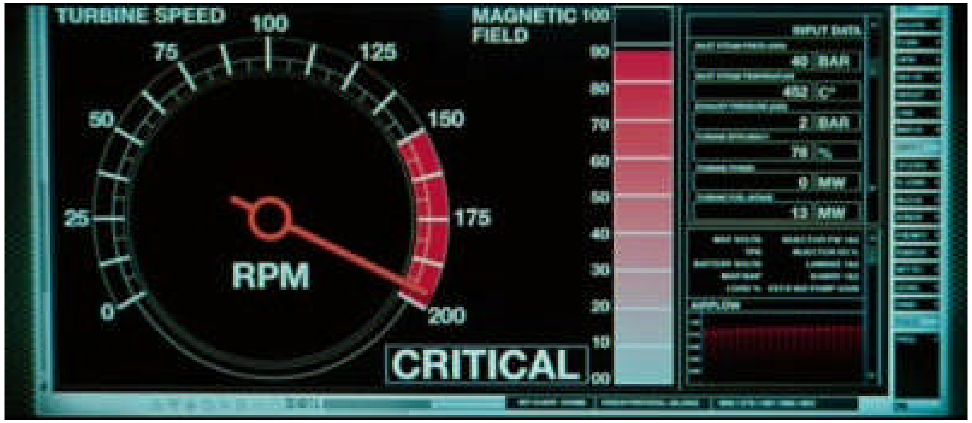




- Later, the two agents penetrate the Kremlin by **hacking the access control system**, forcing it to **validate the authenticity** of their **fake ID token**. They use an autonomous **wireless** device connected to a Smartphone.

Hollywood phy-sec hacking scenes
Mission: impossible - Ghost protocol (2011) ***2/2***

- Inside the Kremlin, they **brute-force a door's keypad** with an extension card connected to a Smartphone.
- They also get into the server room to **control the CCTV and the lifts** of the *Burj Khalifa* hotel (Dubai).

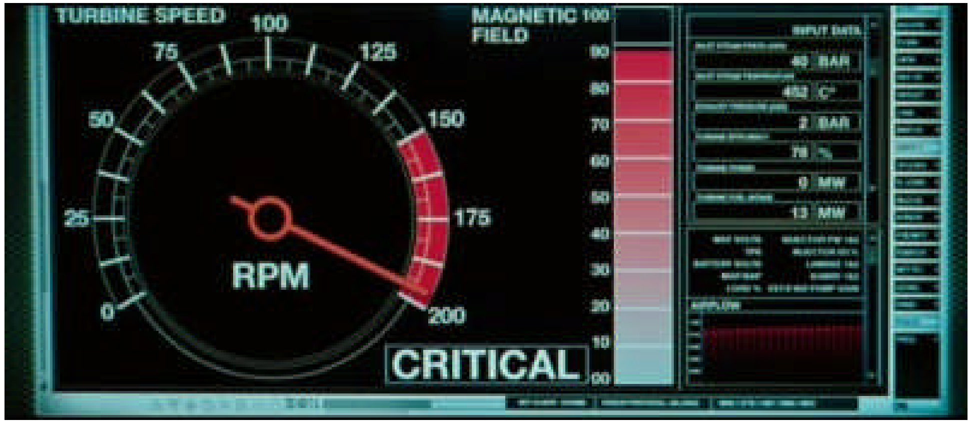


- The **ventilation system** is hacked to slow down (and then speed up) the main turbine of a server room.

Hollywood phy-sec hacking scenes
Mission: impossible - Ghost protocol (2011) ***2/2***

- Inside the Kremlin, they **brute-force a door's keypad** with an extension card connected to a Smartphone. (**Black Hat USA 2012**: My Arduino can beat up your hotel room lock, *Cody Brocious*, later miniaturized in a pen by *SpiderLabs*).

- They also get into the server room to **control the CCTV and the lifts** of the *Burj Khalifa* hotel (Dubai).



- The **ventilation system** is hacked to slow down (and then speed up) the main turbine of a server room.

Agenda

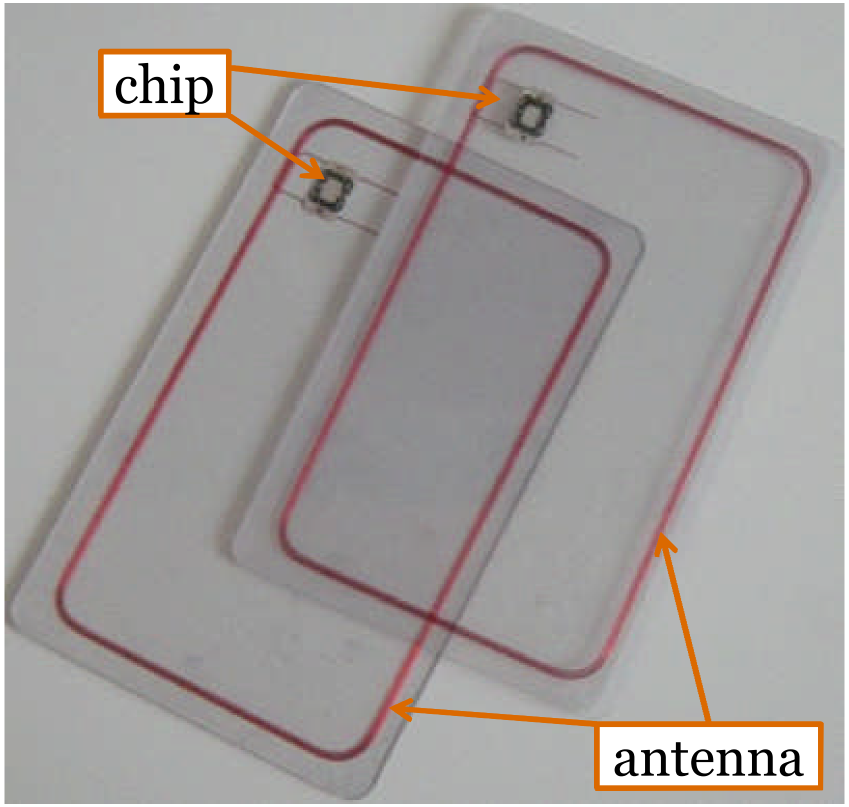
1. Spectacular hacking of doors & cameras in Hollywood movies: fact or fiction?
2. Introducing access control systems, surveillance cameras & video recorders
   a) How they work
   b) What they are made of
3. Existing market solutions and integration issues
   a) The theory - What it should be
   b) In practice - What it actually is
4. Case study: security from the LAN with actual products
   a) Access control systems (eg. Primion)
   b) Digital video recorder (eg. Bosch DiBos)
   c) Air conditioning (eg. Hirovisor)
   d) IP cameras (eg. Axis, Mobotix, Trendnet…)
   e) Other multi-functions systems (eg. Winguard, Winmag plus)
5. Extra risks: hacking the “security” equipment system = 1st step toward the domain admin

Introducing access control systems, surveillance cameras & video recorders

2

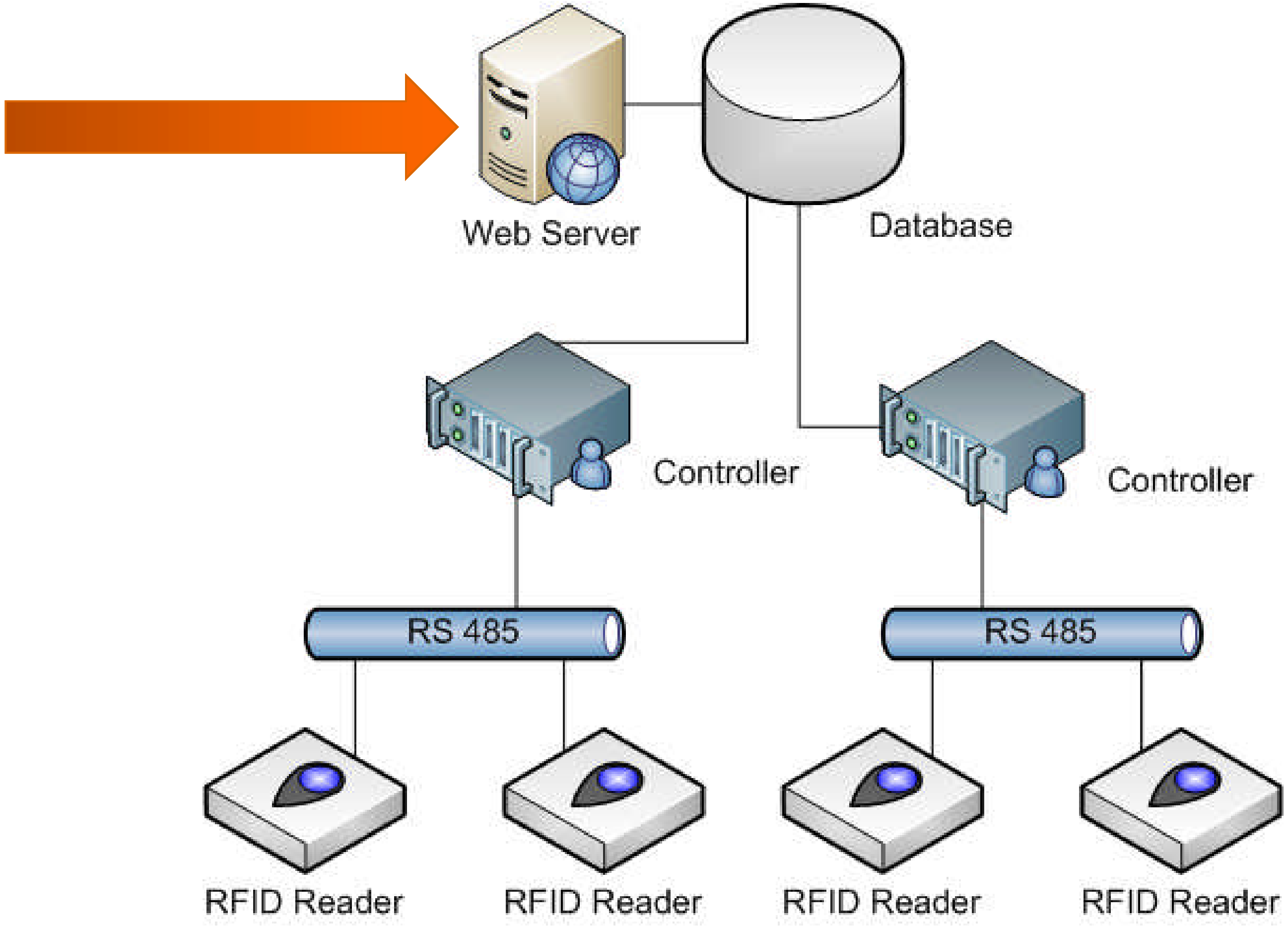
2.a How they work (1/8)

Access control systems



2.a How they work (2/8)

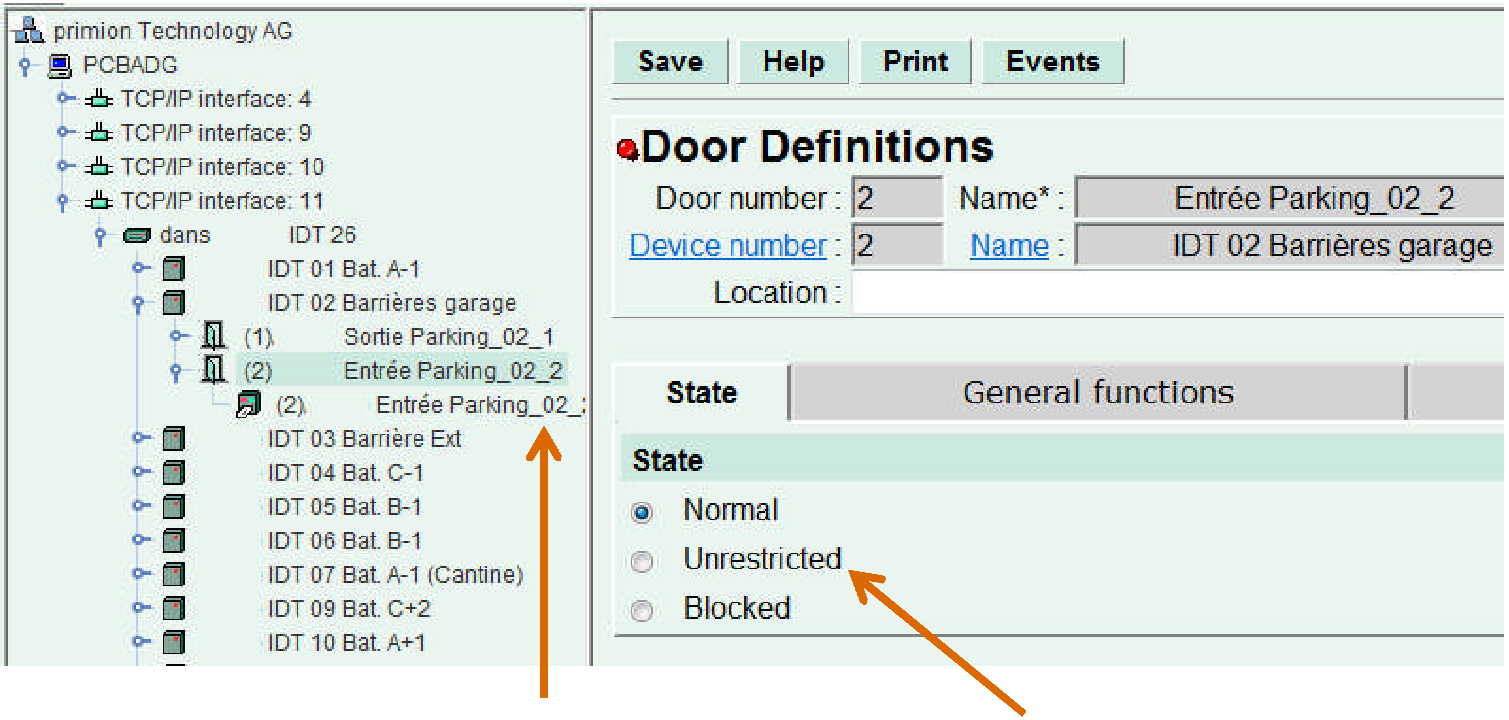
Access control systems



2.a How they work (3/8)

Access control systems

Welcome back in the 90's ☺



- primion Technology AG
  - PCBADG
    - TCP/IP interface: 4
    - TCP/IP interface: 9
    - TCP/IP interface: 10
    - TCP/IP interface: 11
      - dans IDT 26
        - IDT 01 Bat. A-1
        - IDT 02 Barrières garage
          - (1) Sortie Parking_02_1
          - (2) Entrée Parking_02_2
            - (2) Entrée Parking_02_:
        - IDT 03 Barrière Ext
        - IDT 04 Bat. C-1
        - IDT 05 Bat. B-1
        - IDT 06 Bat. B-1
        - IDT 07 Bat. A-1 (Cantine)
        - IDT 09 Bat. C+2
        - IDT 10 Bat. A+1

Door Definitions

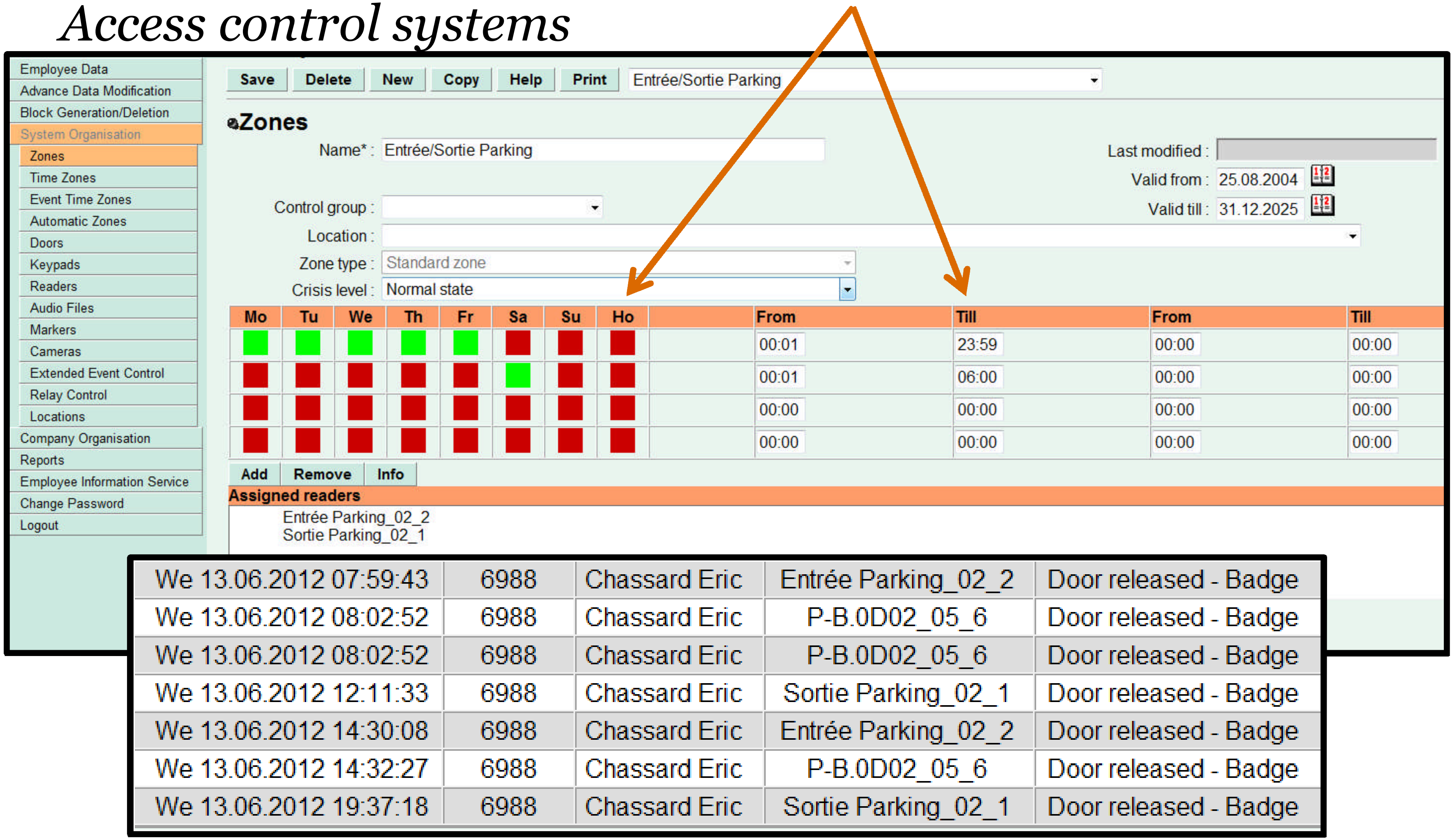
Door number :	2	Name* :	Entrée Parking_02_2
Device number :	2	Name :	IDT 02 Barrières garage
Location :			

State

- ● Normal
- ○ Unrestricted
- ○ Blocked

2.a How they work (4/8)

Access control systems



Entrée/Sortie Parking

Zones

Name* : Entrée/Sortie Parking

Last modified :

Valid from : 25.08.2004

Valid till : 31.12.2025

Control group :

Location :

Zone type : Standard zone

Crisis level : Normal state

Mo	Tu	We	Th	Fr	Sa	Su	Ho	From	Till	From	Till
🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟥	00:01	23:59	00:00	00:00
🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟥	00:01	06:00	00:00	00:00
🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	00:00	00:00	00:00	00:00
🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	00:00	00:00	00:00	00:00

Assigned readers

Entrée Parking_02_2
Sortie Parking_02_1

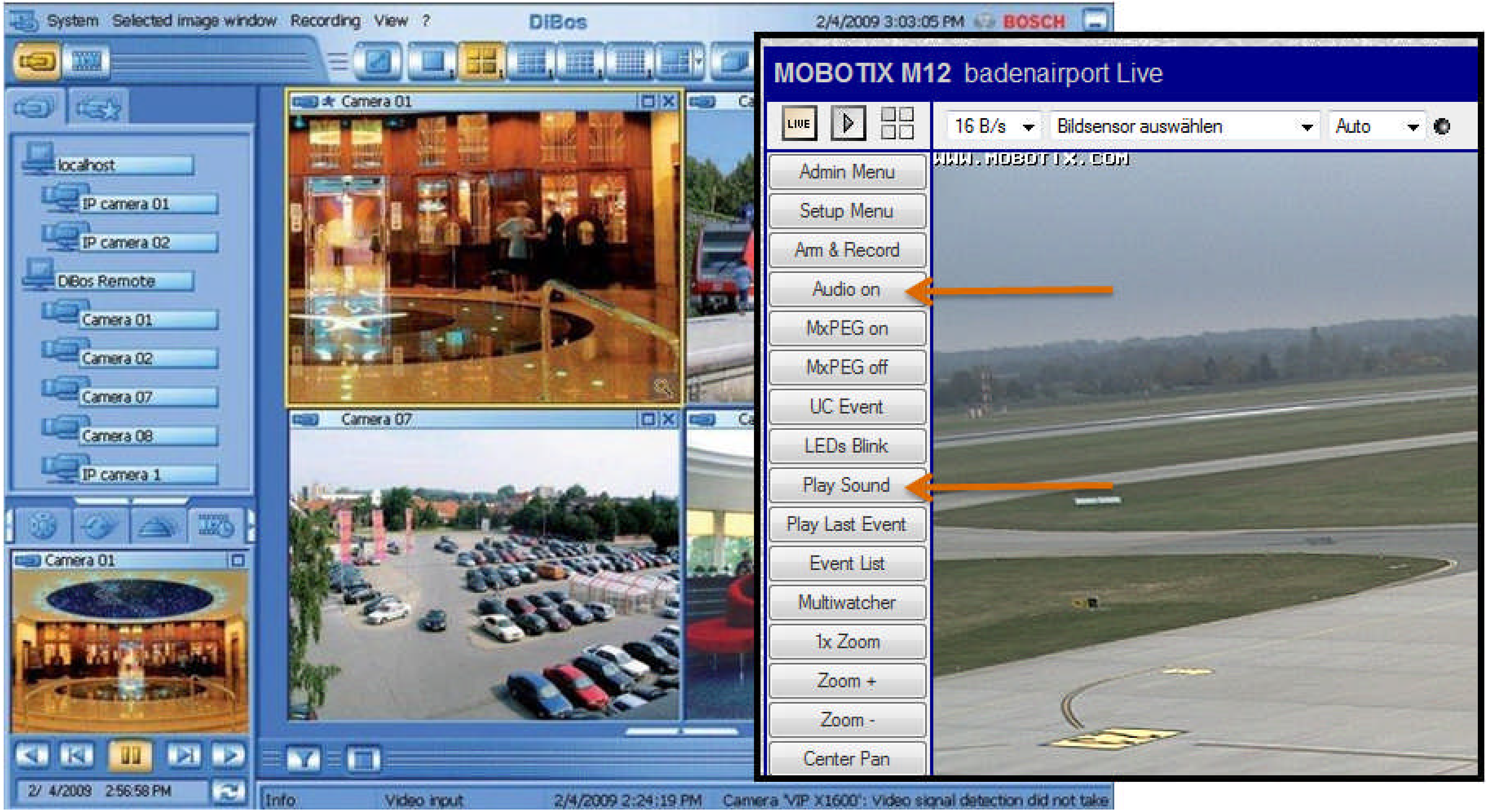
We 13.06.2012 07:59:43	6988	Chassard Eric	Entrée Parking_02_2	Door released - Badge
We 13.06.2012 08:02:52	6988	Chassard Eric	P-B.0D02_05_6	Door released - Badge
We 13.06.2012 08:02:52	6988	Chassard Eric	P-B.0D02_05_6	Door released - Badge
We 13.06.2012 12:11:33	6988	Chassard Eric	Sortie Parking_02_1	Door released - Badge
We 13.06.2012 14:30:08	6988	Chassard Eric	Entrée Parking_02_2	Door released - Badge
We 13.06.2012 14:32:27	6988	Chassard Eric	P-B.0D02_05_6	Door released - Badge
We 13.06.2012 19:37:18	6988	Chassard Eric	Sortie Parking_02_1	Door released - Badge

2.a How they work (5/8)

Surveillance cameras & video recorders

2.a How they work (6/8)

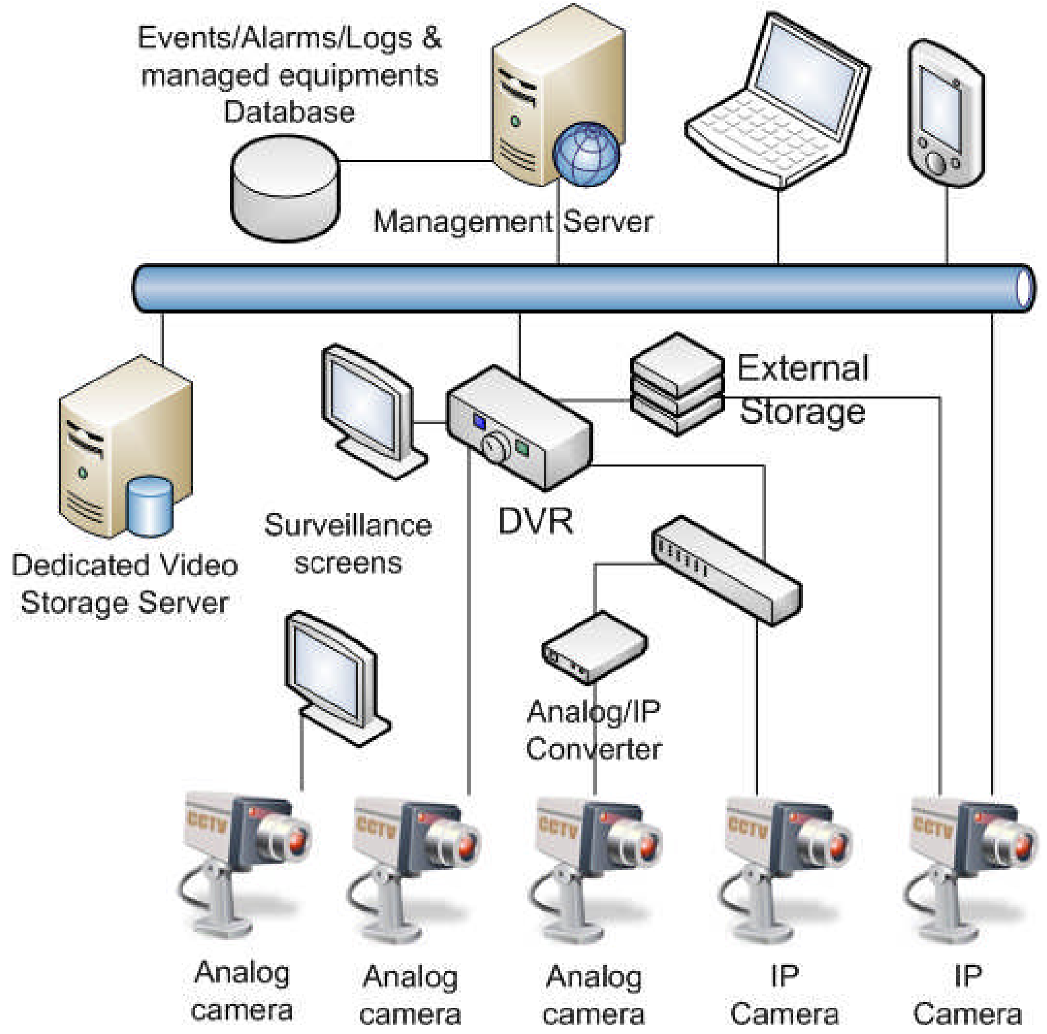
Surveillance cameras & video recorders



Info	Video input	2/4/2009 2:24:19 PM	Camera 'VIP X1600': Video signal detection did not take

2.a How they work (7/8)

Surveillance cameras & video recorders



2.a How they work (8/8)

Surveillance cameras & video recorders

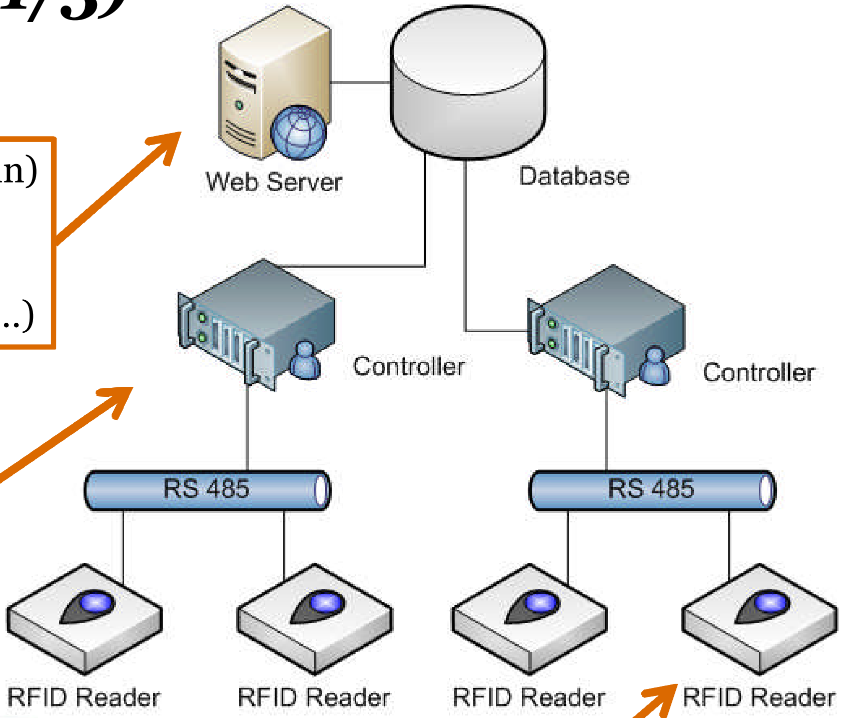
- **Characteristics, example: Bosch IP Camera**
  Integrated web server (+ TLS v1.0)
  Get connected to Video Management System DIBOS, VIDOS, Bosch VMS and to Digital Video Recorders (Divar 700…)
  Need IE>7 and JVM ; ActiveX to install for video visualisation.
  25 simultaneous connections from browsers or 50 connections to VIDOS/VMS
  3 authorisation levels : service, user, live.
  Watermark (to ensure the live or recorded streams have not been altered)
- **Implemented protocols, example: Axis IP Camera**
  IPv4/6, HTTP, HTTPS, QoS Layer 3 DiffServ, FTP, CIFS/SMB, SMTP, Bonjour, UPnP, SNMP v1/v2c/v3(MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS
- **Standardisation attempt, example: ONVIF**
  Sony, Axis, Bosch, Canon, Panasonic, Hitachi, Huawei, Genetec, Dallmeier, Honeywell, Pelco (Schneider Electric)
  → Video standards + SOAP + Web Services

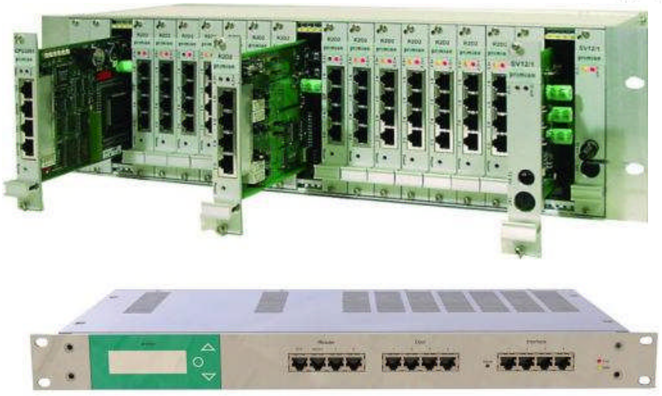
2.b What they are made of (1/3)

Access control systems

- Windows computer (XP… possibly integrated to the Domain) with an all-in-one software setup for the…
- …Open-source or proprietary wide-spread Web-Server (Apache Tomcat) and RDBMS (IBM DB2, MySQL, Postgres…)

- Proprietary, closed-source specific electronics and firmware
- Serial/Ethernet interfaces
- Plug-in cards for more I/O





- RFID chip complying with ISO/IEC14443 Example widespread semiconductor brand: NXP (Philips)
- Proprietary, closed-source specific electronics bringing network connectivity to the reader (and power…)

2.b What they are made of (2/3)

Surveillance cameras & video recorders

Those devices are mainly blackboxes:

- **Digital Video Recorder, example : Bosch Divar XF/700**

  Windows XP SP2 or higher ; Windows Vista SP2 ; Windows 7 (32bits and 64bits)

  Intel Pentium Dual Core, 3.0Ghz

  2 Go RAM

  10 Go Free hard Disk Space

  NVIDIA Geforce 8600 or higher

- **Some other Bosch DVR:**

  Microsoft Windows Storage server 2008

- **Geutebrück Geviscope (successor of the Multiscope):**

  Windows XP embedded

  Windows embedded standard 7

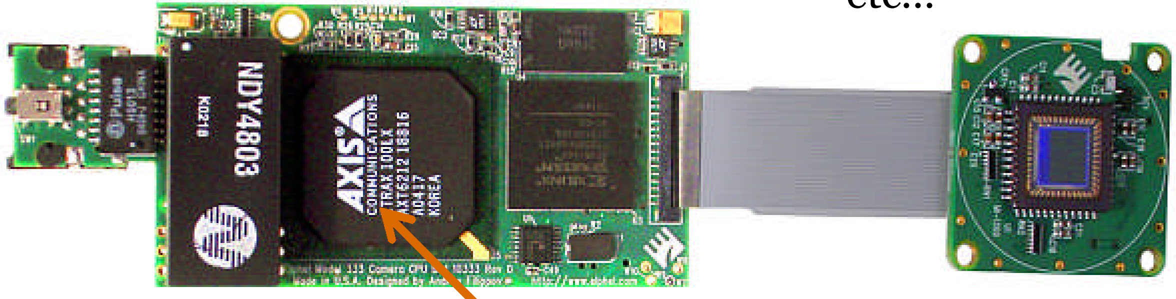
2.b What they are made of (3/3)

Surveillance cameras & video recorders

Firmware based on GNU/Linux… let's read the **licenses details** in the firmware release notes! Who said it was boring? No need to reverse the firmware!

Example: IP Camera Axis M1011 Network Camera 5.20.1 (extract)

GCC library 4.3.1
GNU SASL 0.0.13
Linux kernel 2.6.31
boa 0.94.14
busybox 1.1.3
bwbar 1.2.2
eCos 2.0
tsocks 1.8beta6
nandboot 1.0
stunnel 4.14
ysklogd 1.3
udev 114
glib 2.22.4
gst-plugins-base 0.10.14
iproute2 2.6.15-060110
iptables 1.4.0
gst-plugins-good 0.10.17
gstreamer 0.10.26
libaccess 0.0.1
libelf 0.8.10
libiconv (extracted from glibc) 2.4
libnl 1.1
ethtool 6
mtdutils 1.0.1
etc…

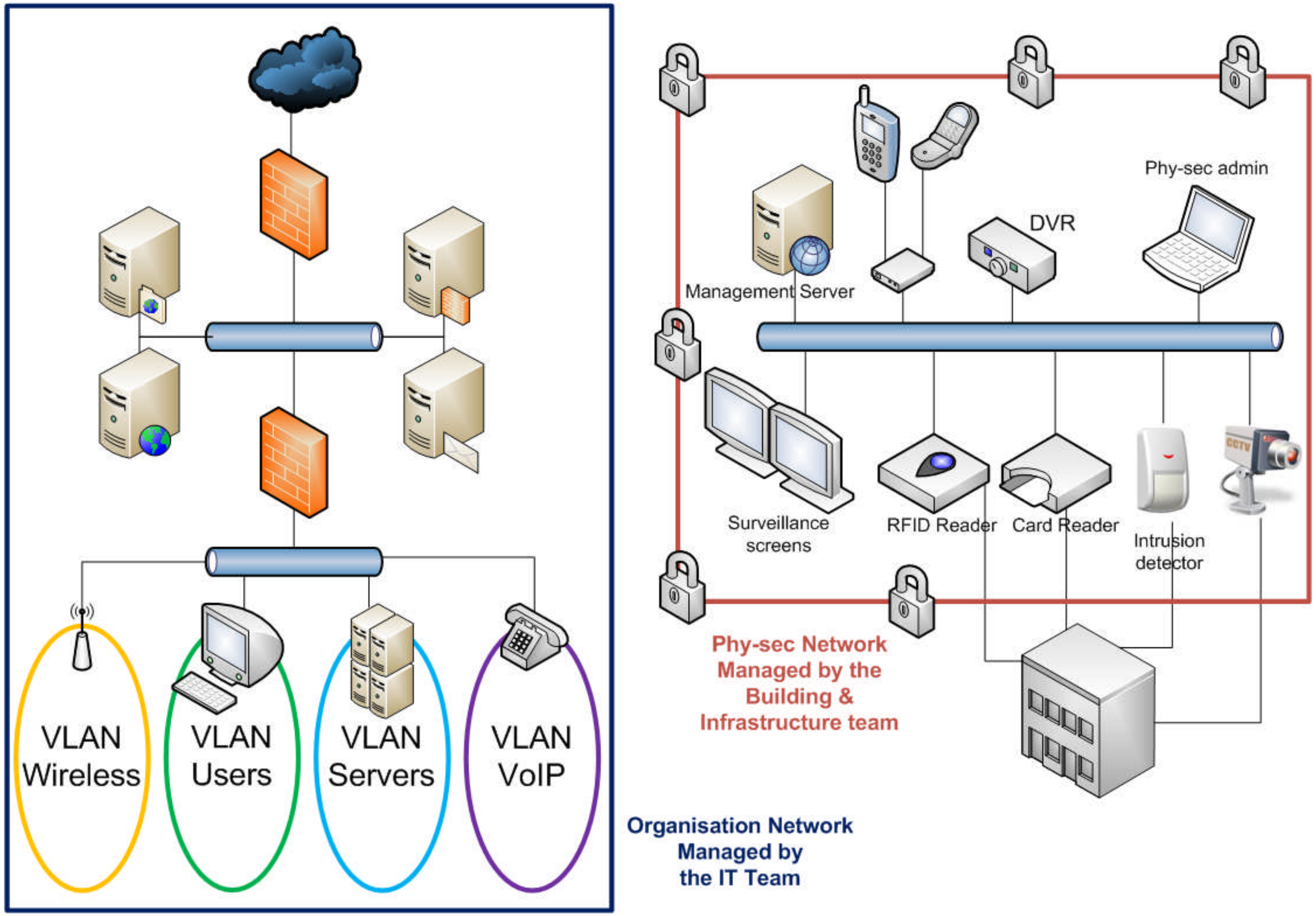


ETRAX 100LX : 32-bit RISC @100MHz
Axis Code Reduced Instruction Set (CRIS)

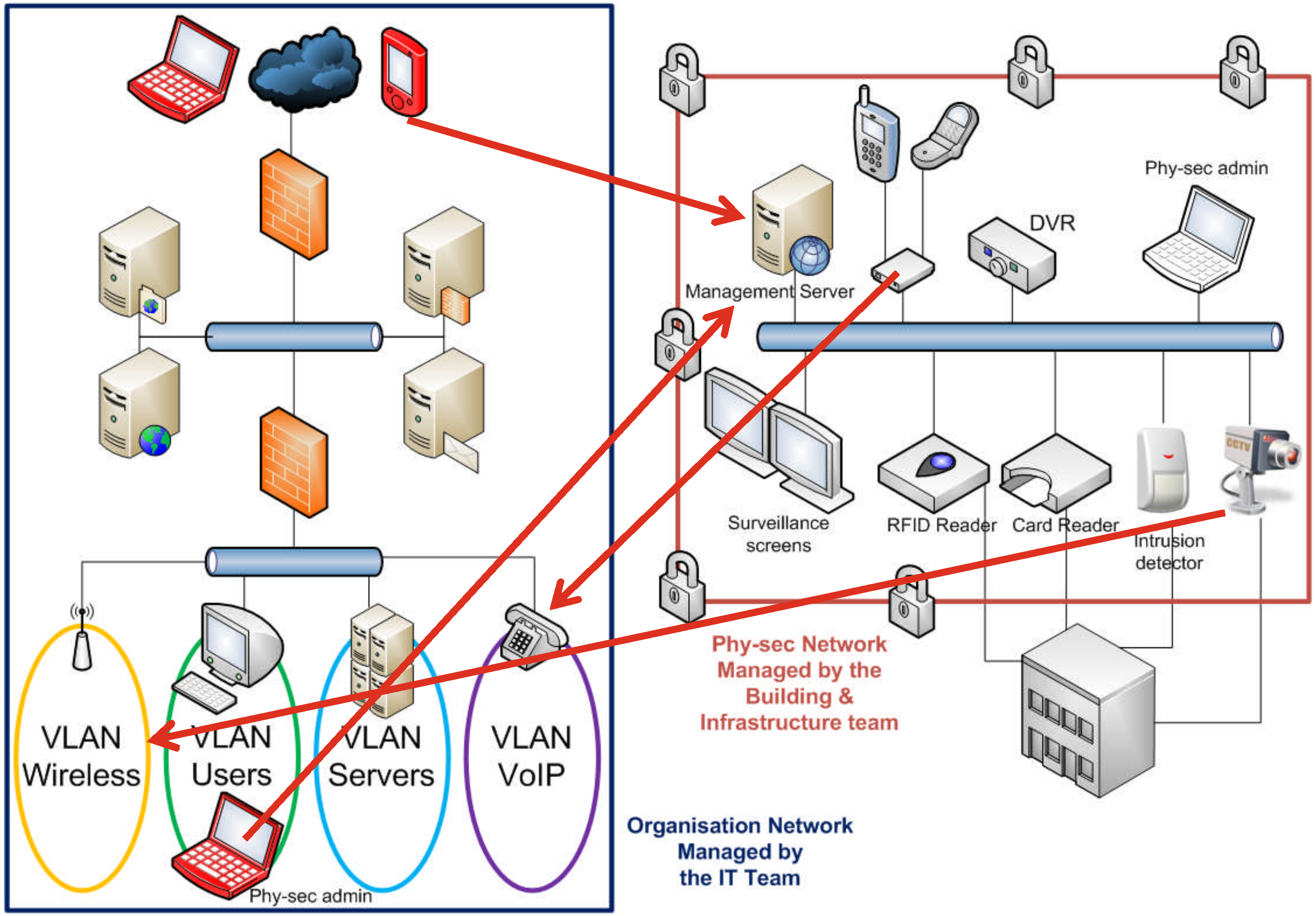
Existing market solutions and integration issues

3

3.a The theory - What it should be



3.b In practice - What it actually is (1/5)



3.b In practice - What it actually is (2/5)

Convenience/negligence/marketing → security issues

The network is **not hermetic anymore**… excepted, maybe, for the **IT Security best practices**:

System protections

- No Antivirus scans,
- No password policies,
- No least privileges principle,
- No updates…

Network protections

- No Firewall,
- No Access Control Lists,
- No IDS,
- No VLAN segregation…

3.b In practice - What it actually is (3/5)
Existing market solutions possibilities

Considering the previous explanations on the network integration of the Phy-sec solutions, those movies' scenes shouldn't seem **so unrealistic** anymore.

Finally, commercial arguments from manufacturers and editors websites are other elements that should catch your attention on their solutions :

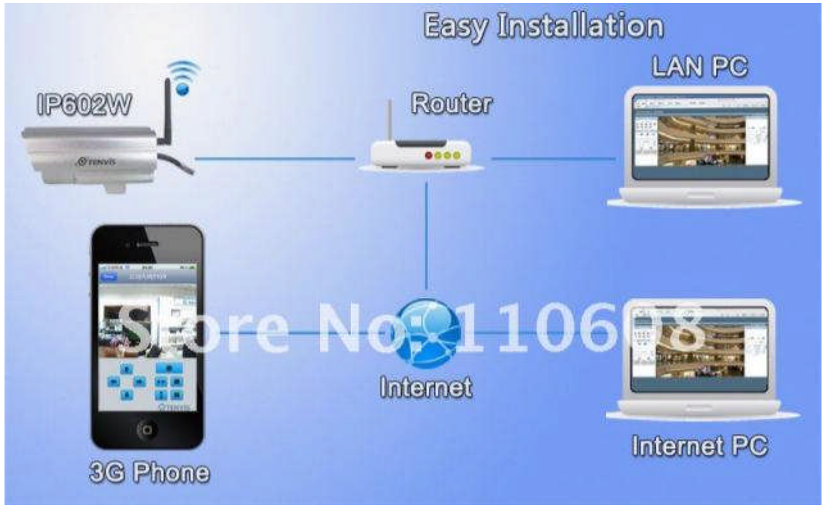
"You can do everything with our **all-in-one** technology/solution/software... By accessing a single computer/software/web page, you can **manage every equipment** of the **whole physical security infrastructure**..."

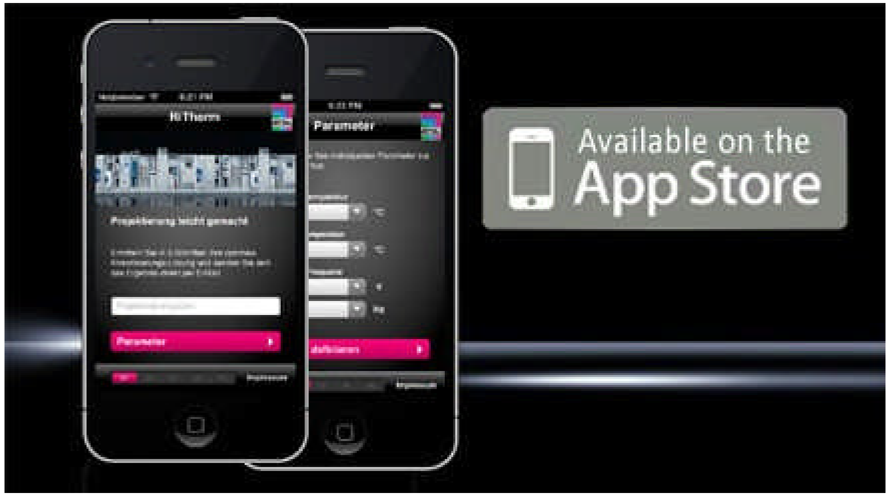
"You can do everything on your LAN... But also remotely, **from the Internet**."

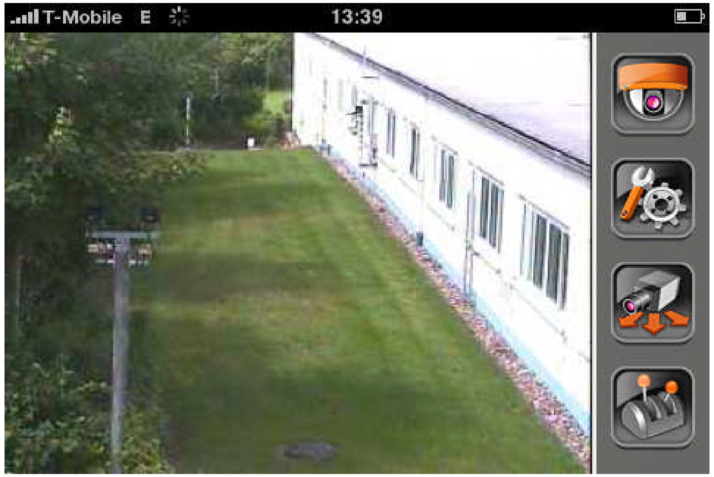
"You can use your Smartphone/Tablet to **wirelessly and remotely** manage your infrastructure".

3.b In practice - What it actually is (4/5)

Mobile applications for phy-sec management

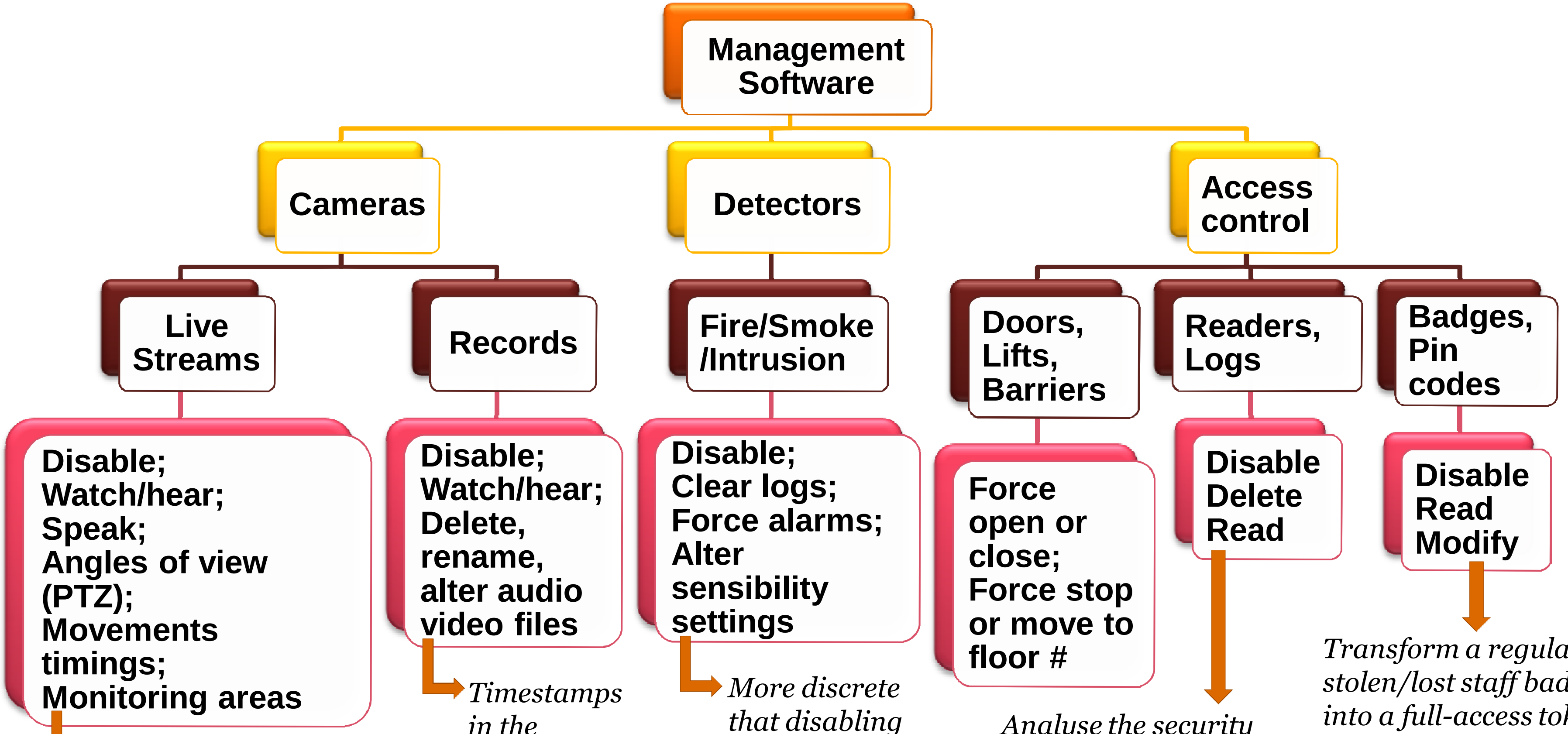






3.b In practice - What it actually is (5/5)

All-in-one solutions' possibilities



Management Software

Cameras

Live Streams

Disable; Watch/hear; Speak; Angles of view (PTZ); Movements timings; Monitoring areas

Find a path to follow to avoid triggering the alarm and the recording

Records

Disable; Watch/hear; Delete, rename, alter audio video files

Timestamps in the files' names

Detectors

Fire/Smoke /Intrusion

Disable; Clear logs; Force alarms; Alter sensibility settings

More discrete that disabling

Access control

Doors, Lifts, Barriers

Force open or close; Force stop or move to floor #

Readers, Logs

Disable Delete Read

Analyse the security guards' patrols, paths, habits and timings

Badges, Pin codes

Disable Read Modify

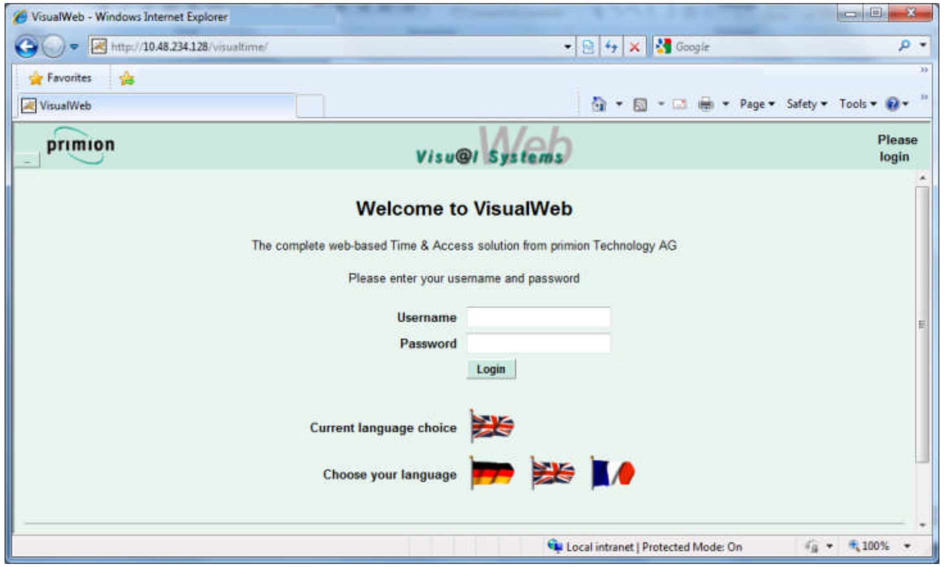
Transform a regular stolen/lost staff badge into a full-access token

DoS: de-authorise a specific badge on a specific door…

Case study: security from the LAN with actual products

4

4.a Access control (eg. Primion) (1/5)


VisualWeb - Windows Internet Explorer
http://10.48.234.128/visualtime/
Google
Favorites
VisualWeb
Page ▾ Safety ▾ Tools ▾
primion
Visu@l Systems Web
Please login
Local intranet | Protected Mode: On
100%

Welcome to VisualWeb

The complete web-based Time & Access solution from primion Technology AG

Please enter your username and password

Username

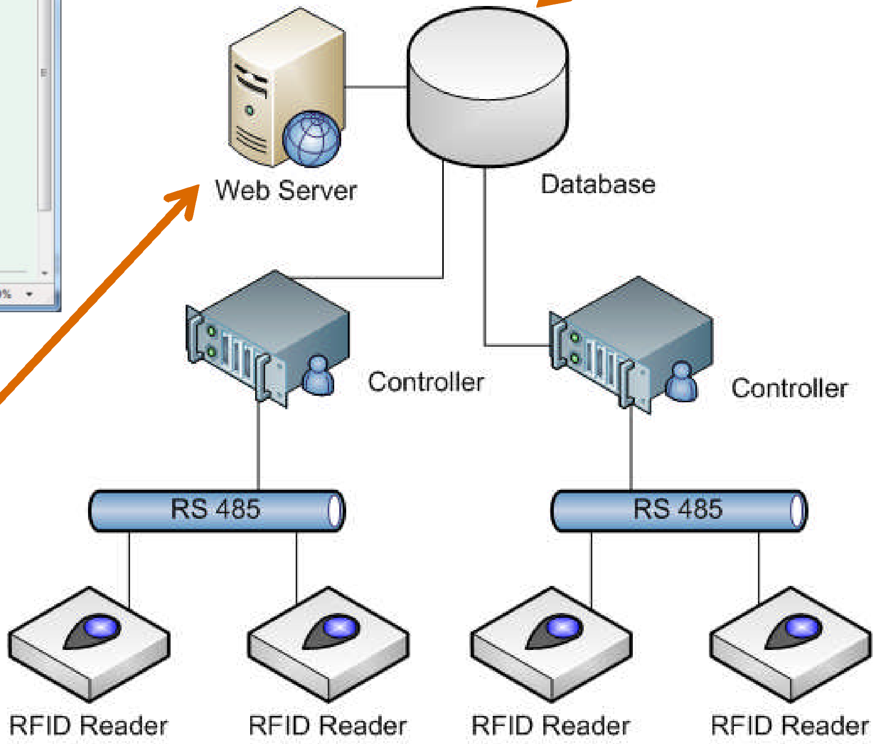
Password

Login

Current language choice

Choose your language

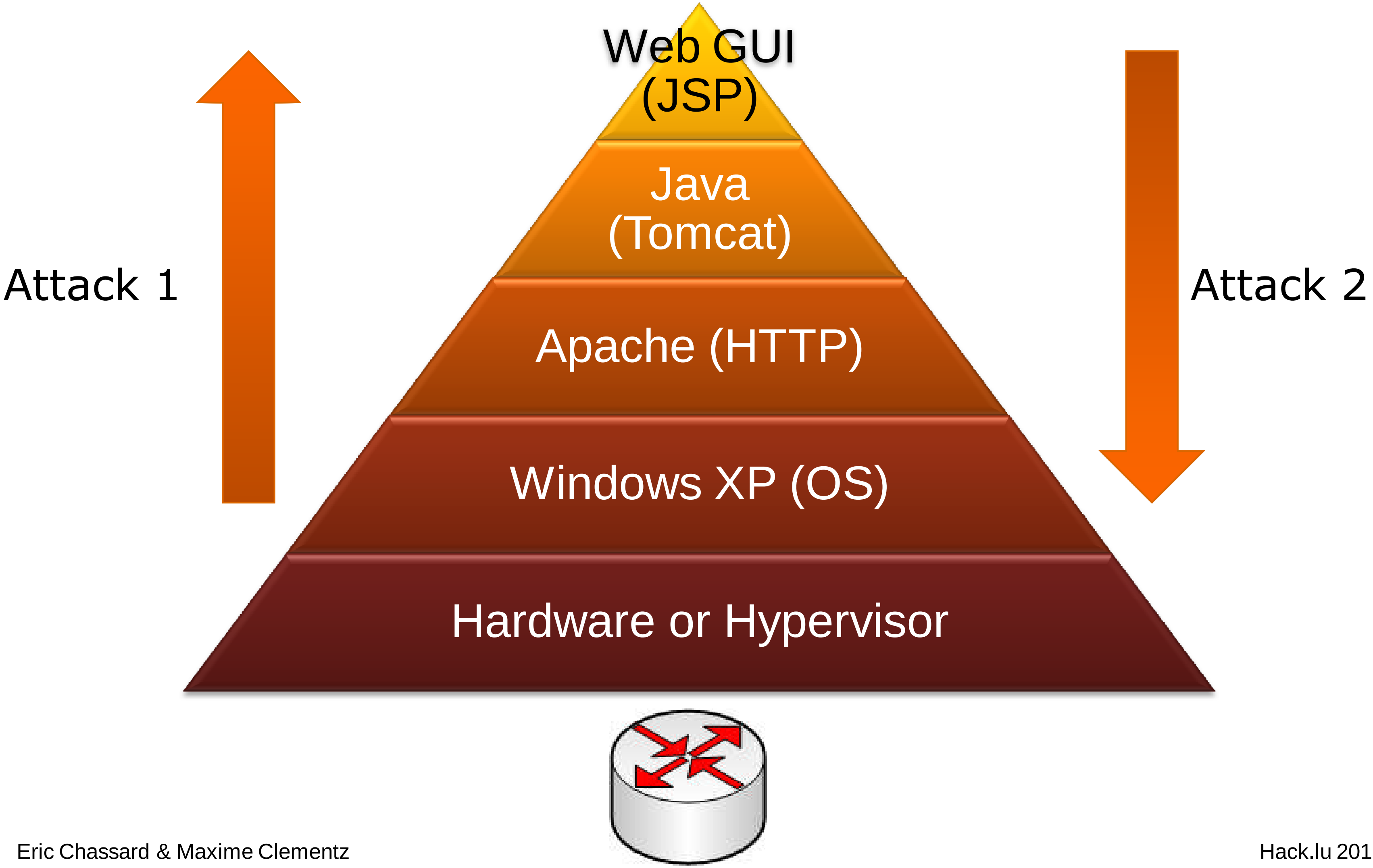
- IBM DB2 9.1



- Windows XP (or Windows Server 2003, Standard Edition SP1)
- HTTP(S) : Apache TomCat 4.1.24* running with **local admin privileges**
- MS-RDP

* Apache Tomcat 4.1.24 was released in 2003 !

4.a Access control (eg. Primion) (2/5)



Attack 1

Web GUI (JSP)

Java (Tomcat)

Apache (HTTP)

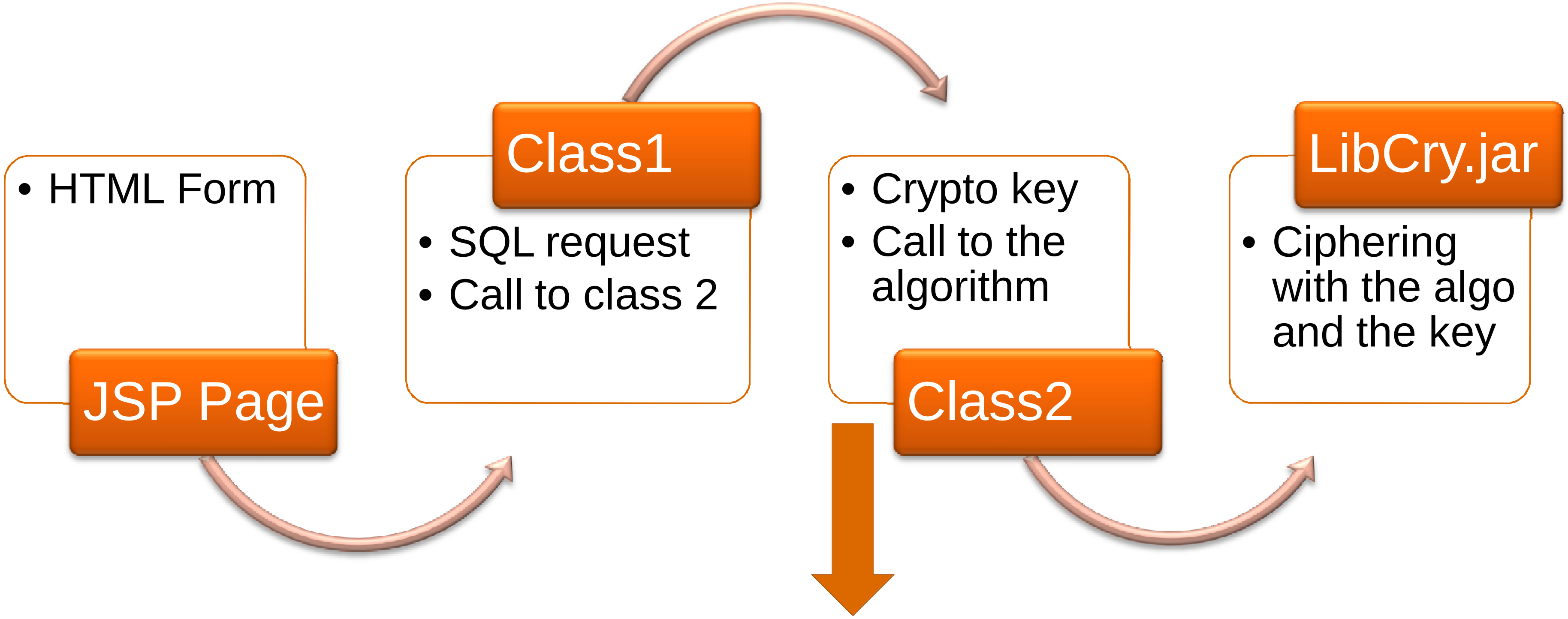
Windows XP (OS)

Hardware or Hypervisor

Attack 2

4.a Access control (eg. Primion) (3/5)

Attack 1: From Windows to the Web GUI



JSP Page
- HTML Form

Class1
- SQL request
- Call to class 2

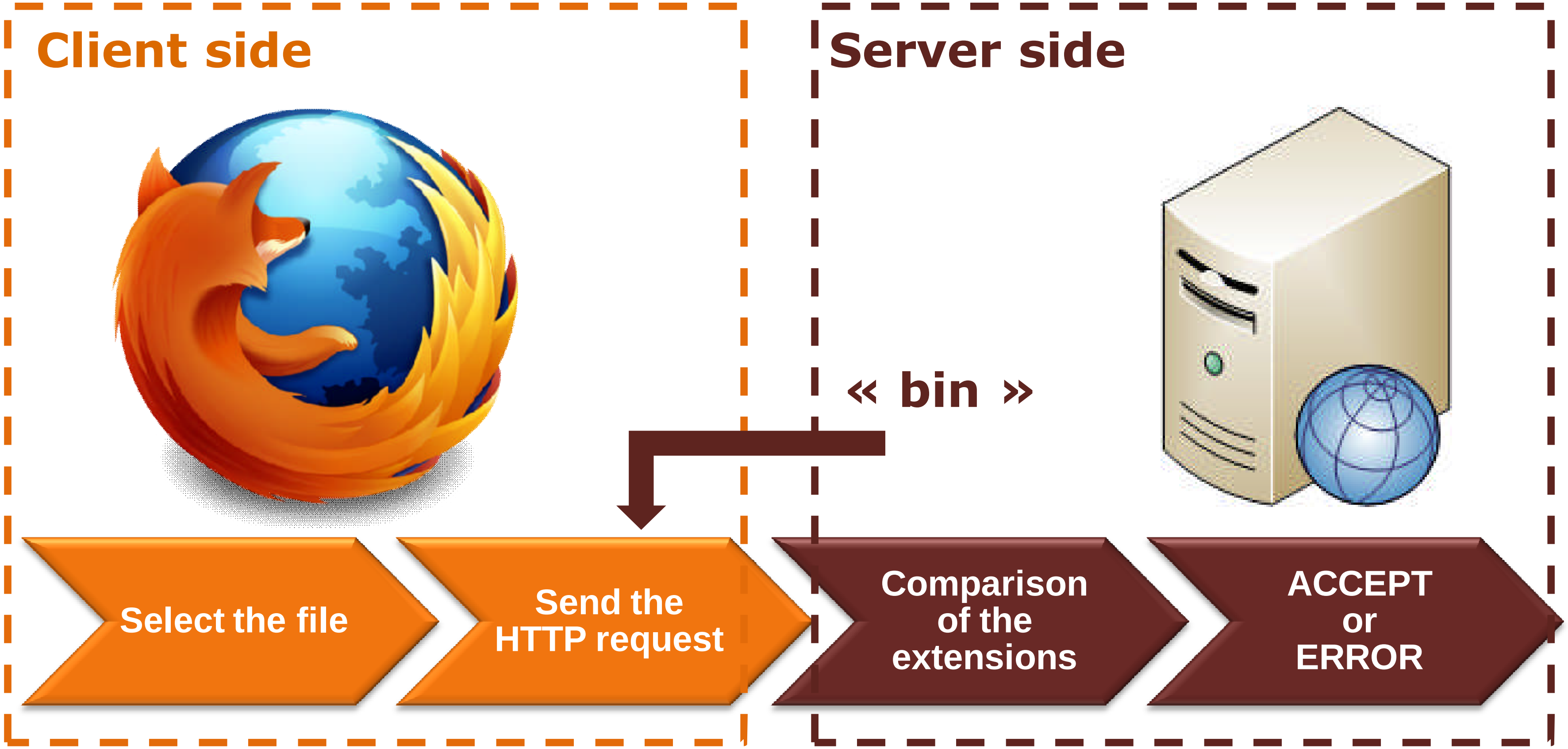
Class2
- Crypto key
- Call to the algorithm

LibCry.jar
- Ciphering with the algo and the key

The stored form of the passwords could be MD5(SHA1(**p**)) but by **default** it is: **3DES**(**p**, **unique_key**)

4.a Access control (eg. Primion) (4/5)

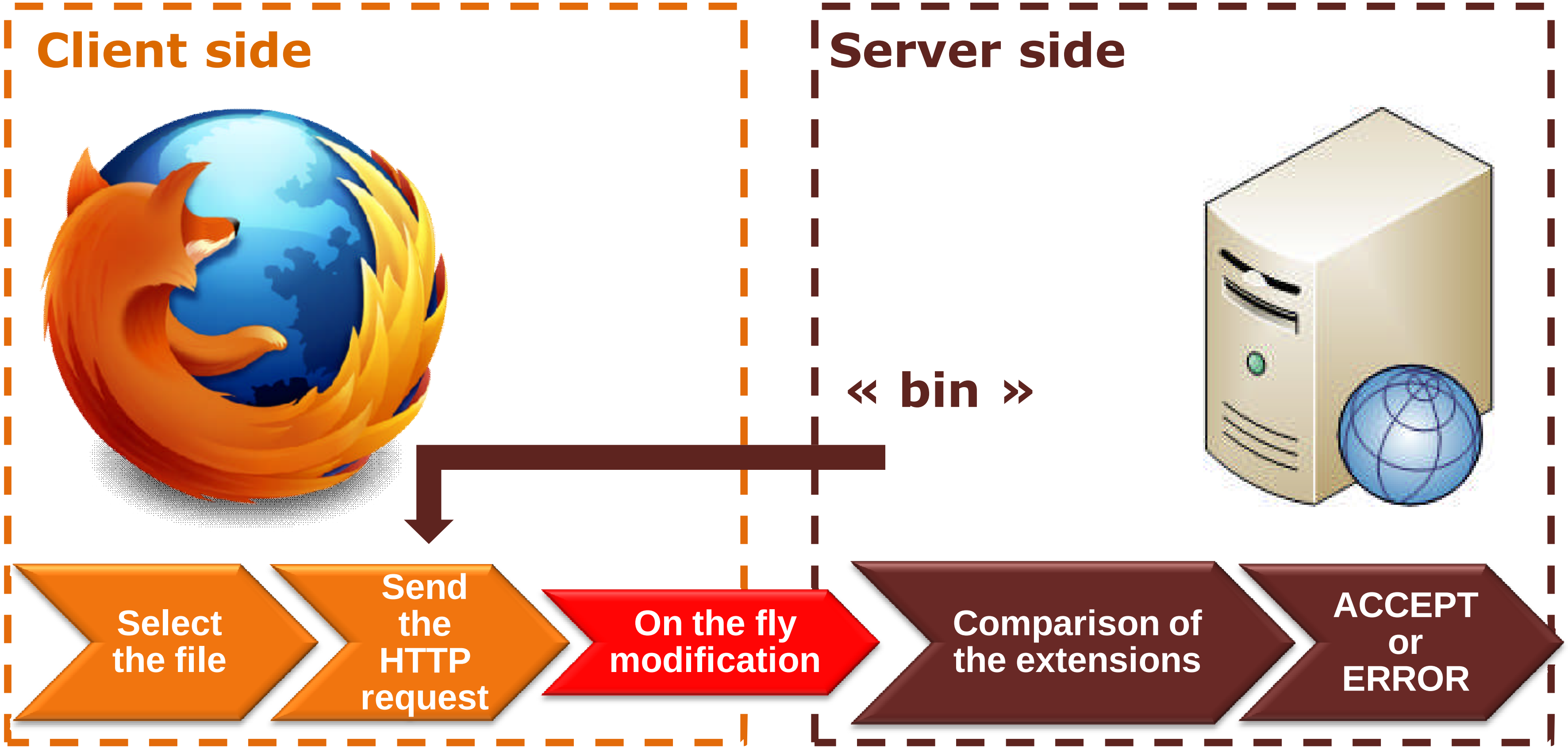
Attack 2: From the Web GUI to the Windows system



- Extension in request = bin
- Extension of the file

4.a Access control (eg. Primion) (5/5)

Attack 2: From the Web GUI to the Windows system



Client side

Server side

« bin »

Select the file

Send the HTTP request

On the fly modification

Comparison of the extensions

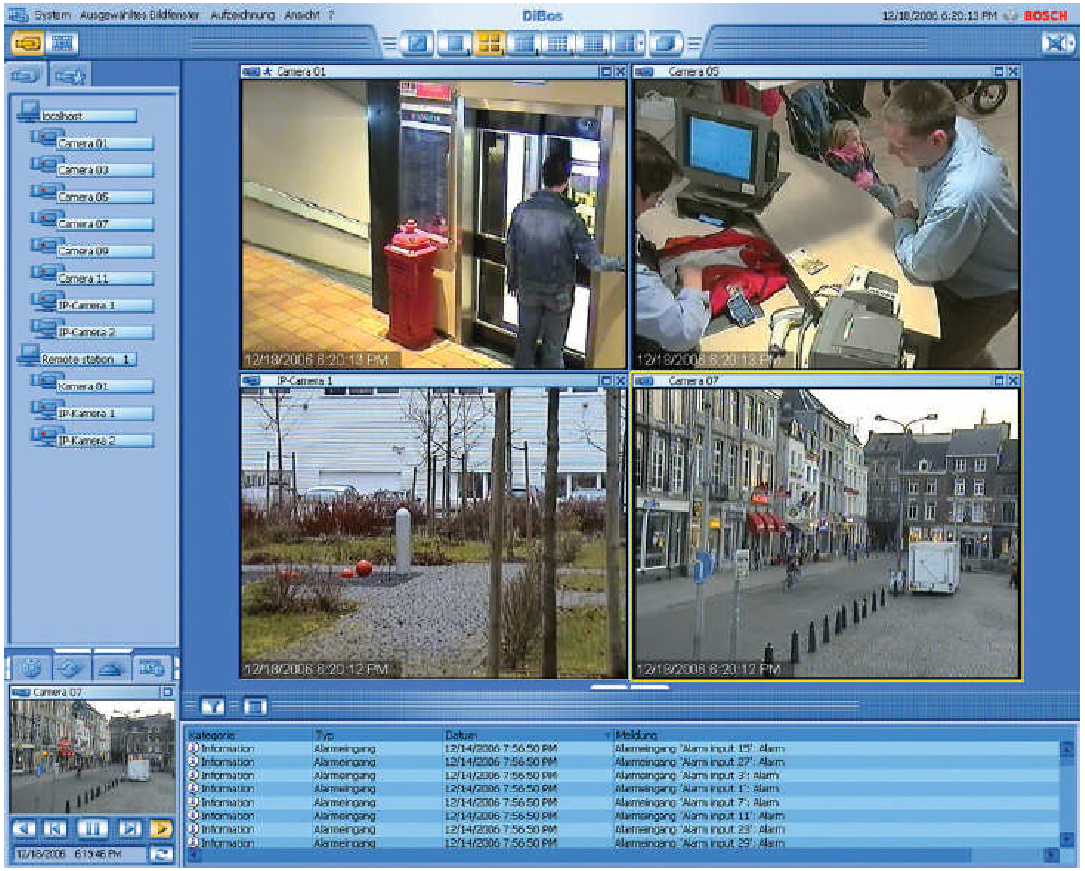
ACCEPT or ERROR

- Extension in request = jsp
- Extension of the file

4.b Digital video recorder

Bosch DiBos

- Web interface (http)
- MS-RDP
- **Weak** credentials
- **Bypass** shell restrictions
- Application runs with **local Admin privilege**



Kategorie	Typ	Datum	Meldung
Information	Alarmeingang	12/14/2006 7:56:50 PM	Alarmeingang 'Alarm input 15': Alarm
Information	Alarmeingang	12/14/2006 7:56:50 PM	Alarmeingang 'Alarm input 27': Alarm
Information	Alarmeingang	12/14/2006 7:56:50 PM	Alarmeingang 'Alarm input 3': Alarm
Information	Alarmeingang	12/14/2006 7:56:50 PM	Alarmeingang 'Alarm input 1': Alarm
Information	Alarmeingang	12/14/2006 7:56:50 PM	Alarmeingang 'Alarm input 7': Alarm
Information	Alarmeingang	12/14/2006 7:56:50 PM	Alarmeingang 'Alarm input 11': Alarm
Information	Alarmeingang	12/14/2006 7:56:50 PM	Alarmeingang 'Alarm input 23': Alarm
Information	Alarmeingang	12/14/2006 7:56:50 PM	Alarmeingang 'Alarm input 29': Alarm

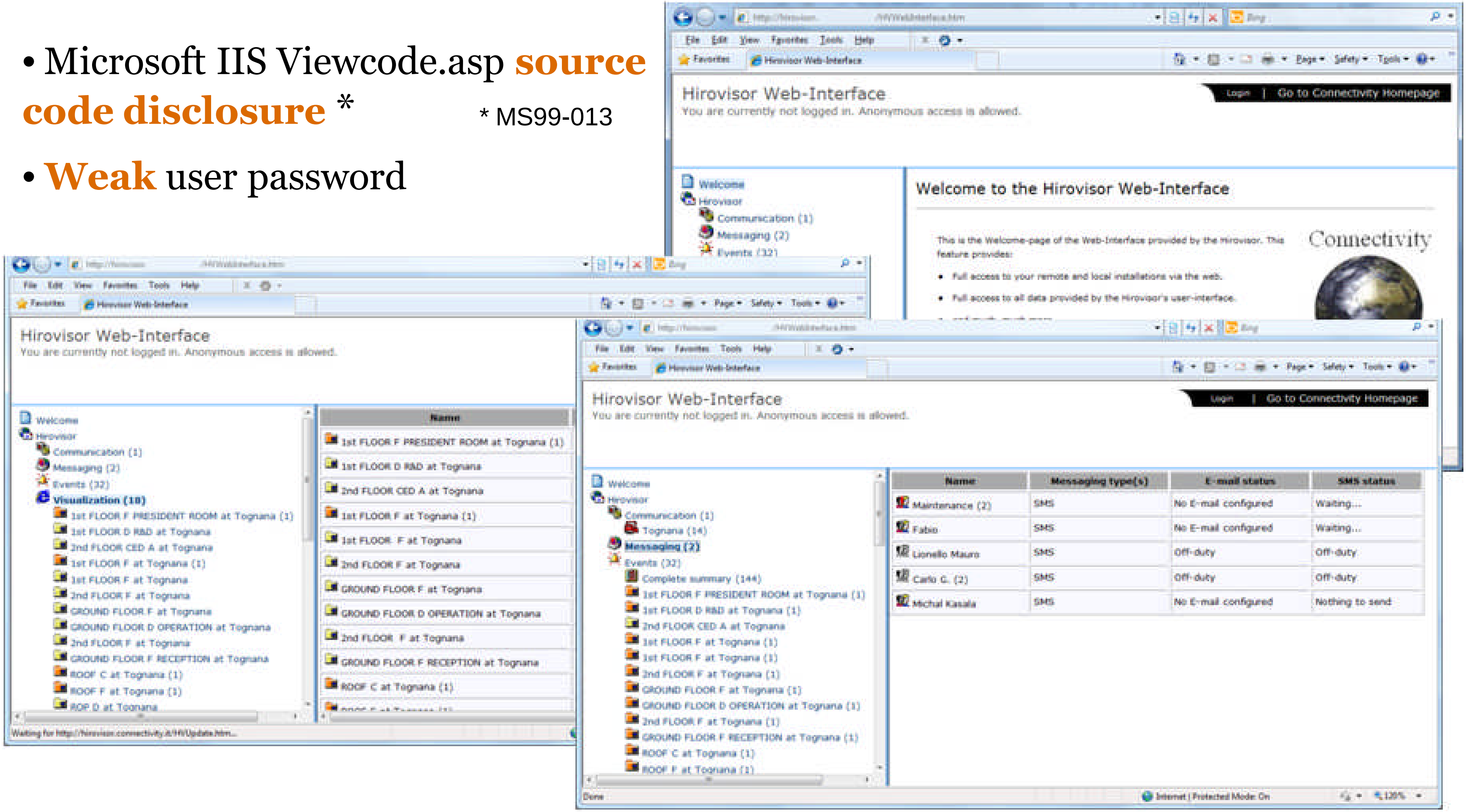
4.c Air conditioning (eg. Hirovisor) 1/2

Hirovisor Web-interface

- Microsoft IIS Viewcode.asp **source code disclosure** *

- **Weak** user password

* MS99-013



Hirovisor Web-Interface

You are currently not logged in. Anonymous access is allowed.

Welcome to the Hirovisor Web-Interface

This is the Welcome-page of the Web-Interface provided by the Hirovisor. This feature provides:

- Full access to your remote and local installations via the web.
- Full access to all data provided by the Hirovisor's user-interface.

Name
1st FLOOR F PRESIDENT ROOM at Tognana (1)
1st FLOOR D R&D at Tognana
2nd FLOOR CED A at Tognana
1st FLOOR F at Tognana (1)
1st FLOOR F at Tognana
2nd FLOOR F at Tognana
GROUND FLOOR F at Tognana
GROUND FLOOR D OPERATION at Tognana
2nd FLOOR F at Tognana
GROUND FLOOR F RECEPTION at Tognana
ROOF C at Tognana (1)

Name	Messaging type(s)	E-mail status	SMS status
Maintenance (2)	SMS	No E-mail configured	Waiting...
Fabio	SMS	No E-mail configured	Waiting...
Lionello Mauro	SMS	Off-duty	Off-duty
Carlo G. (2)	SMS	Off-duty	Off-duty
Michal Kasala	SMS	No E-mail configured	Nothing to send

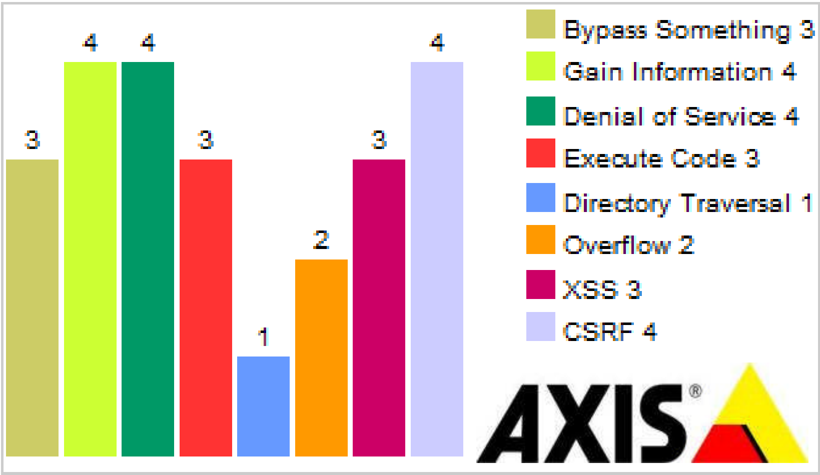
Waiting for http://hirovisor.connectivity.it/HI/Update.htm...

Login | Go to Connectivity Homepage
Welcome
Hirovisor
Communication (1)
Messaging (2)
Events (32)
Visualization (18)
1st FLOOR F PRESIDENT ROOM at Tognana (1)
1st FLOOR D R&D at Tognana
2nd FLOOR CED A at Tognana
1st FLOOR F at Tognana (1)
1st FLOOR F at Tognana
2nd FLOOR F at Tognana
GROUND FLOOR F at Tognana
GROUND FLOOR D OPERATION at Tognana
2nd FLOOR F at Tognana
GROUND FLOOR F RECEPTION at Tognana
ROOF C at Tognana (1)
ROOF F at Tognana (1)
ROOF D at Tognana
Tognana (14)
Complete summary (144)
Connectivity
Hirovisor Web-Interface
File Edit View Favorites Tools Help
Favorites
Page Safety Tools
Done
Internet | Protected Mode: On
120%

4.d IP Camera vulnerabilities

Entry point to the LAN ?

Vulnerabilities By Type

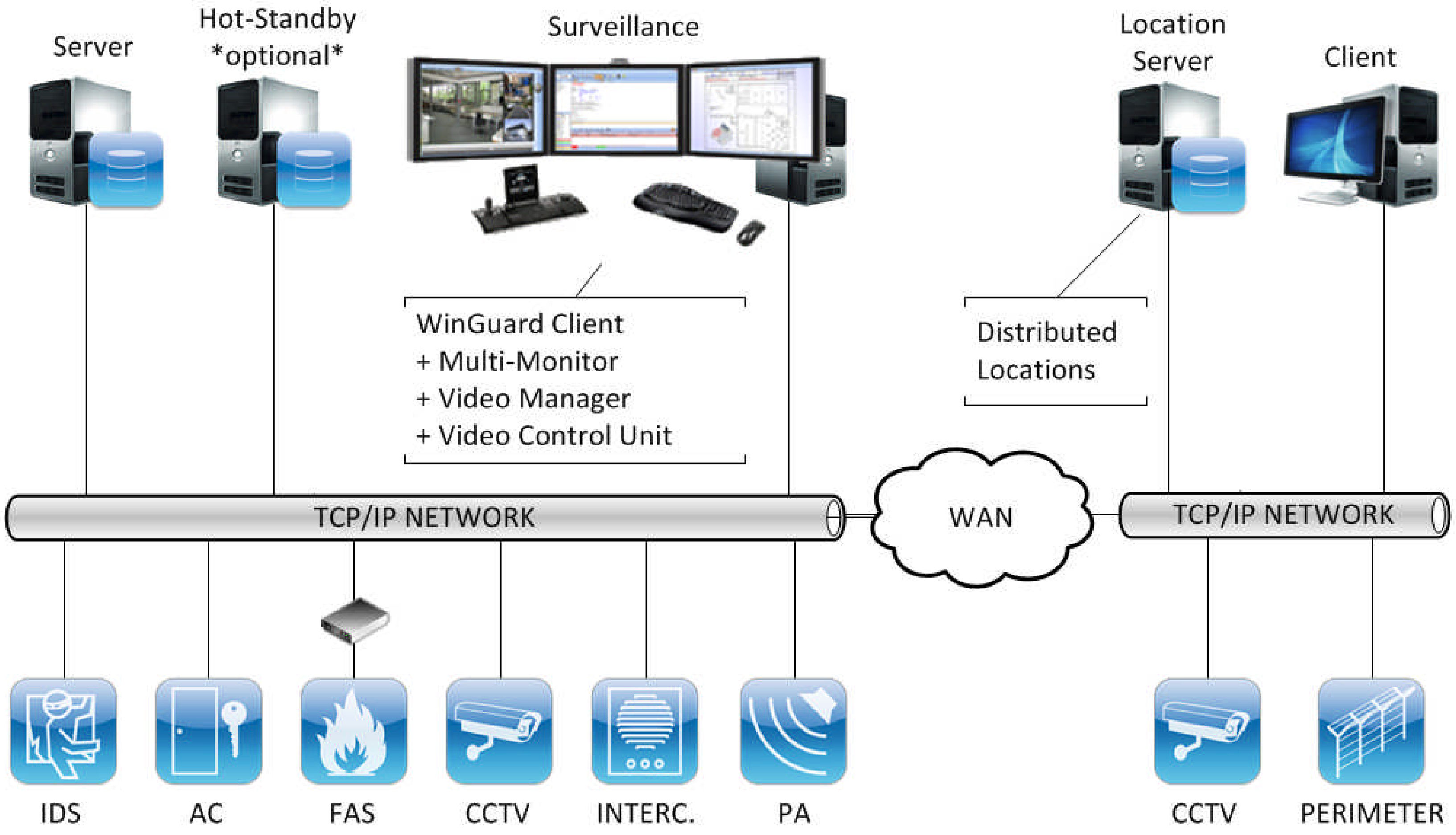


Non-exhaustive list of known vulnerabilities:

- **Axis**: authentication bypass, infoleak: **clear text passwords** for DDNS, FTP, SMTP servers, remote code execution… (*cvedetails*);
- **Mobotix**: XSS (*cvedetails*);
- **Trendnet**: Infoleak, unprotected video streams (*console-cowboys.blospot.com*) and code execution (*cvedetails*);
- **12+ brands** with the same flaw in the "Hi35xx" chipset: authentication bypass, infoleak: **clear text passwords** for DDNS, FTP, SMTP, alarms servers… (*Don Kennedy*);
- Those devices can be found using **Google dorks** and **Shodan**.

4.e Other multi-functions systems (1/4)

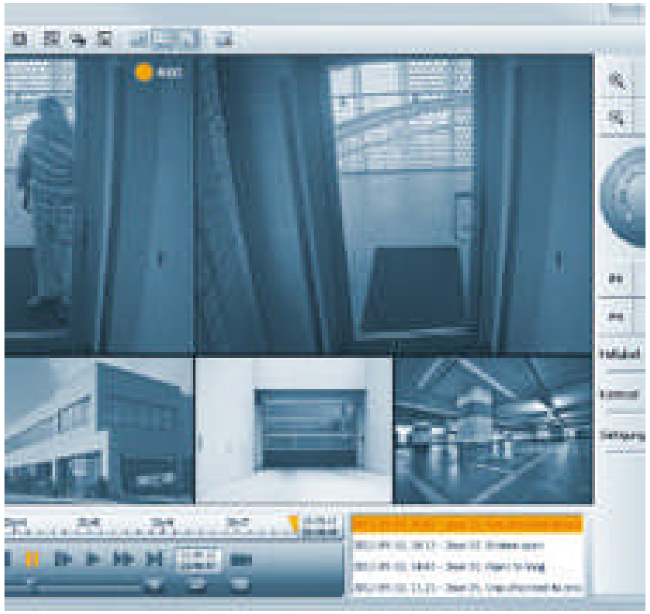
Winguard



4.e Other multi-functions systems (2/4)

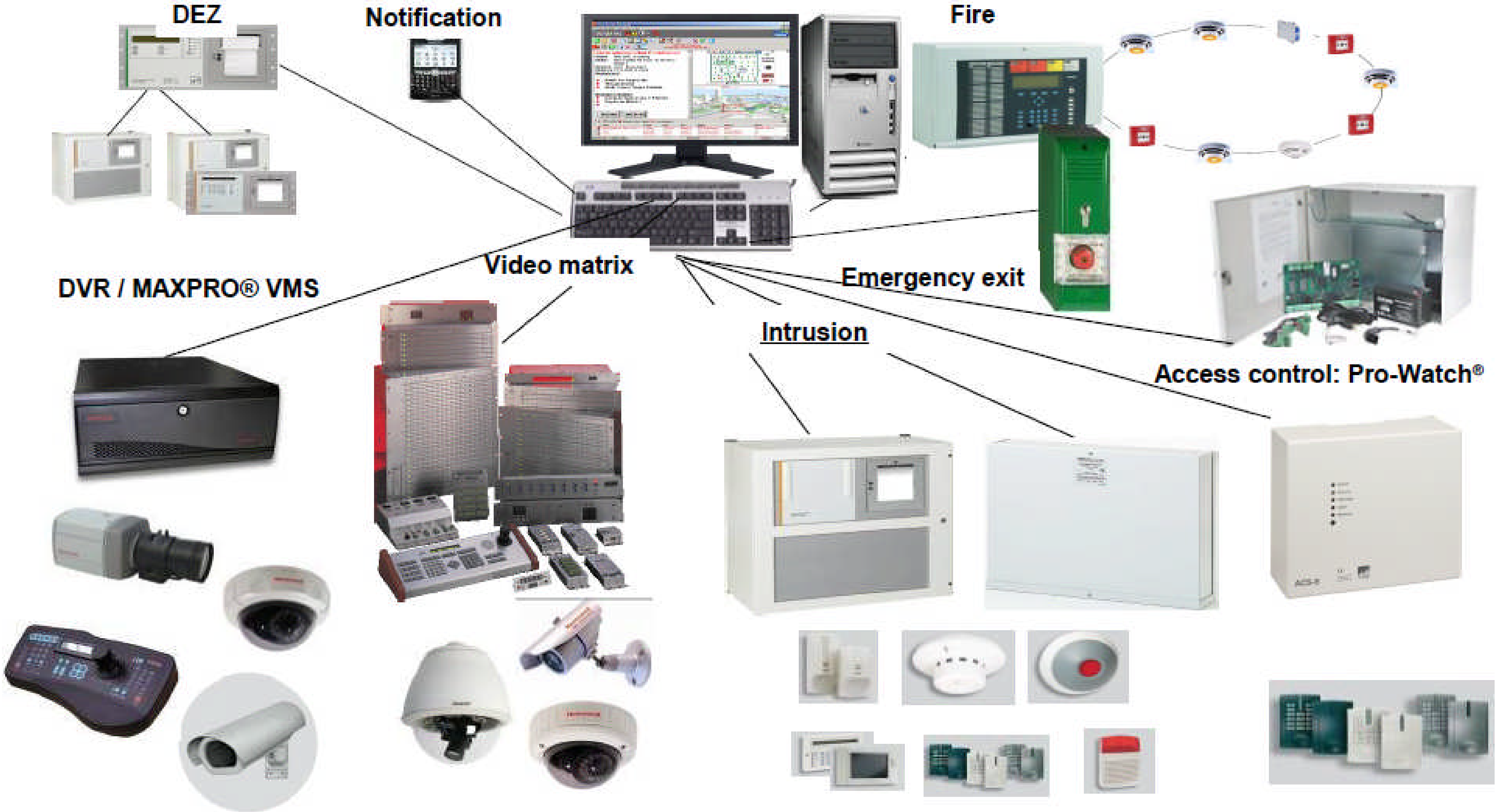
Winguard

- Windows Server 2003, Standard Edition SP2
- Services: HTTP(S) (Tomcat 6), MS-SQL 9.0, Winguard (tcp/1234)
- Apache Tomcat Manager **common administrative credentials**
→ .war deployment → Shell
- Tomcat running with **System privileges**
- **Weak** vendor credentials



4.e Other multi-functions systems (3/4)

WinMag Plus



4.e Other multi-functions systems (4/4)

WinMag Plus

- Windows Server 2003, Standard Edition SP2
- Services: HTTP (IIS6+ASP.Net), MS-RDP, WinMag Plus
- **Weak** vendor credentials
- Local dababases (.mdb) contains **unencrypted credentials**

Extra risks: hacking the “security” equipment system = 1st step toward the domain admin

5

5. Real life case study

Some of these software :

- Run on Windows
- …with the **privileges** of the local **Admin** account
- …which is a member of the corporate **Domain**
- …whose the **Admin** account is used to launch **weekly** AV scans on every computer

➔ The Domain Admin credentials are **locally stored** in memory (and updated on a regular basis, thanks to the AV Scan…)

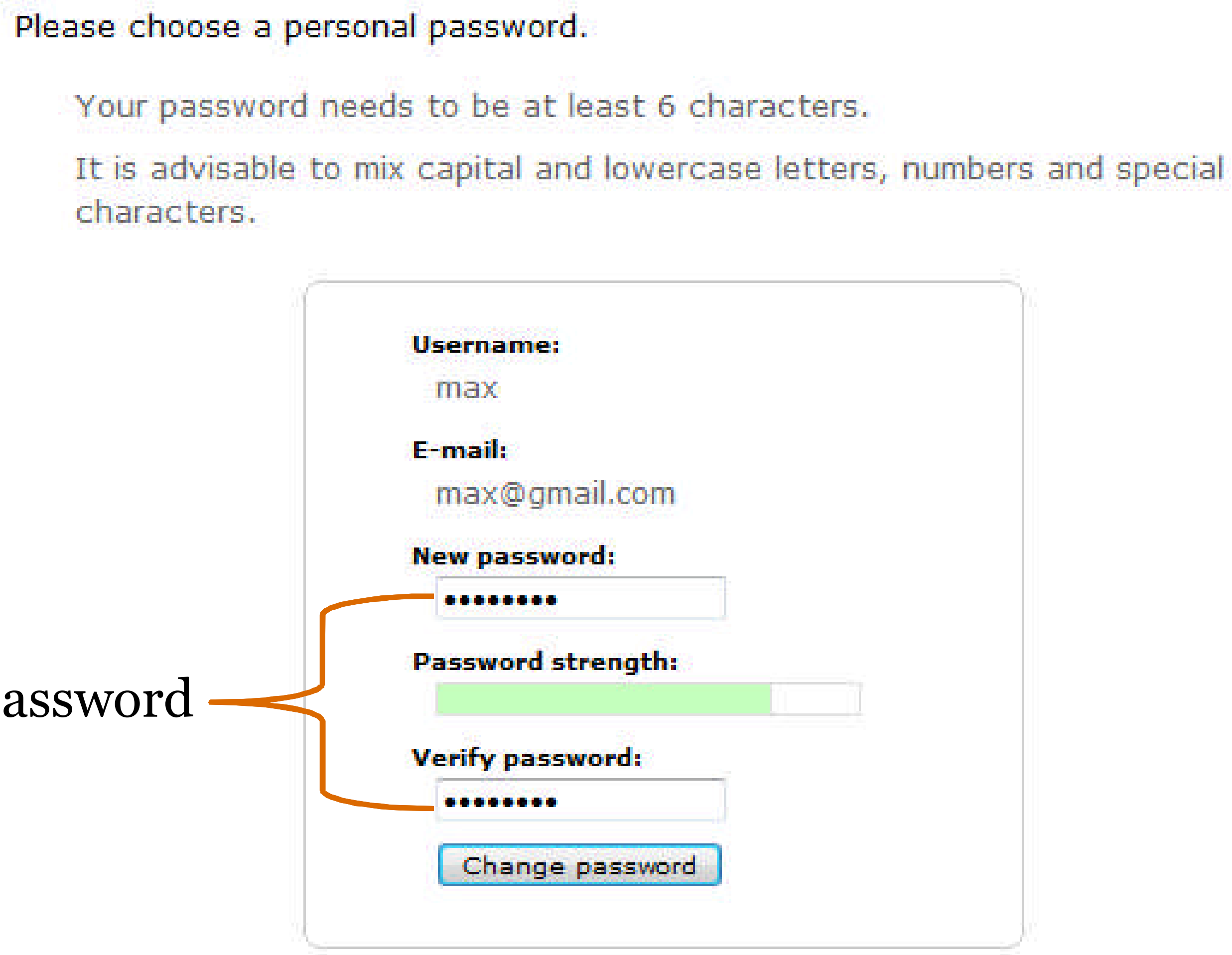
➔ Those credentials could be retrieved via the privileges of the software suffering a "Remote Code Execution" **vulnerability**

Conclusion

- **Well-known, widely spread and mature** technologies
- “Basic” / “not so complex” security flaws
- **Standards** and **best practices** according to physical security, **not** IT security.
- Physical security **assessments** rely on physical security **≠** IT security.
- Phys-sec admin **≠** IT-sec admin.
- No communication between Facilities/Infrastructure and IT teams.
- Issues may be **may known** and the customer may be aware of **the risks** but **finally decides** to deploy/expose on the LAN for more **convenience**.

Fun fact

From a security vendor website inscription form



Please choose a personal password.

Your password needs to be at least 6 characters.

It is advisable to mix capital and lowercase letters, numbers and special characters.

Username:
max

E-mail:
max@gmail.com

New password:
●●●●●●●●

Password strength:

Verify password:
●●●●●●●●

password